The CIO Security Sub Committee (CIOSS) had its December meeting on the 13th.

Attending:

Larry Grund - DPS, Chairmen
Greg Fay - DAS
Linda Torgeson - IDOT
Jennifer Eubanks - Treasury
Pat Martin - Treasury
John Wolf - IWD
Lesa Quinn - DID
Kevin Kammermeier - DIPS

Discussion revolved around the definitions of a Risk Assessment, Vulnerability Assessment, and a Security Audit. We determined that the committee would review the definitions below and advise both Larry Grund and Greg Fay by the 17th.

Risk Assessment

> A process that systematically identifies valuable system resources and threats to those resources (known and postulated), quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence and identifies potential impact resulting from the loss of information or capabilities of a system. The analysis lists risks in order of cost and criticality, thereby determining where counter measures should be applied first. It is usually financially and technically infeasible to counteract all aspects of risk, and so some residual risk will remain, even after all available counter measures have been deployed.

Vulnerability Assessment

> 1) An examination of the ability of a system or application, including current security procedures and controls, to withstand assault. 2) Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation, which includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount that attack.

Security Audit

> An independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for counter measures. The basic audit objective is to establish accountability for system entities that initiate or participate in security-relevant events and actions. Thus, means are needed to generate and record security audit trail and to review and analyze the audit trail to discover and investigate attacks and security compromises.

It was decided that Greg would provide a copy of the Risk Assessment document for committee review within one week. The committee will have the responsibility to review the document by the January meeting. It is the goal of the committee to have the DAS Security team begin the risk assessment process with approximately 60 departments/agencies.

A tentative draft schedule of events appears in the attached PDF.

Next meeting is scheduled for January 10, 2005 - Wallace Building 3rd West 1/2 conference room.